Windows® Document Signing with PrivaSeal™

James S. Prohaska
David R. Auman
Aliroo, Inc.

PKI Technical Working Group
August 12, 1999 Meeting

Corporate Mission

Provide comprehensive, easy-to-use solutions
for every dimension
of enterprise document security
and content assurance

Issues with Digital Signatures

- Have to be Easy to Use and Apply
  - A signed document must be recognized by everyday users.
  - Average User must be able to easily sign and verify.
  - Complementary to EXISTING Work Processes.
    - Multiple Signatures
    - Digital Certificate Verification
    - Integral to working documents

Issues with Digital Signatures

- Implementation Cost
  - Cost of Implementing a PKI
    - Full Internal PKI
    - Commercial based PKI
  - Cost of issuing Tokens
  - Cost of Certificates
  - Administrative Cost

Issues with Digital Signatures

Need a flexible product that minimizes the barriers to:

⇒ Ease of Use ⇐

⇒ Cost and Level of PKI Implementation ⇐

⇒ Cost of Issuance and Management ⇐

In order to encourage adoption of Digital Signatures

PrivaSeal™

Document Content Assurance

Signing and Verification System

that combines

Digital Certificate

with a

Personal Autograph

Enterprise Security and Document Content Assurance

Aliroo™

PrivaSeal Features

- Uses Signing Object combining Digital Certificate with signers autograph
- Drag and Drop Document Signing; Click to Verify
- X.509 V3 compliant
- Suitable for personal or enterprise use
- Legal acceptance in most states

PrivaSeal Features

- Compatible with Windows-Based OLE/RTF applications
- SmartCard, USB, PSN and Windows SN Token Support
- Supports Multiple Signatures on a single document
- True-type font scaling of signer’s autograph
- Supports Issuance of signing object

PrivaSeal™ Components

- PrivaSeal Signature Editor
  - Issuance of Signature Object
- PrivaSeal Signer
  - Applies signature to document
- PrivaSeal Verifier
  - Verifies document and signer

PrivaSeal™ Issuance

- Issuance of Signing Object
  - Binds certificate, autograph, token, credentials and object properties through digital signature of the issuer
- Corporate Issuance Model
  - Signing object signed by corporate authority
- Individual Issuance Model
  - Self-signed signing object

PrivaSeal™ Signature Editor

- Imports Issuer’s X.509 Certificate
- Imports Signer’s X.509 Certificate
- Imports/edits bitmap of signer’s autograph
- Converts bitmap to true-type font
- Establishes token assignment and signing object credentials and properties
- Generates issuer-signed signing object

PrivaSeal™ Signer

- PrivaSeal Signer signs and applies signing credentials to Document - Drag and Drop or Plug-in
- Selective signing of RTF based upon signing object properties
- Multiple signatures are order dependent, previous signatures signed as part of the document
- Supports re-signing and viewing of certificate chain and signing object properties

PrivaSeal™ Signer - Tokens

- Supports Variety of Smart Card Tokens
  - PC/SC and Proprietary Smart Card Readers
  - ISO 7816 compliant smart cards
  - Simple ID token with PIN
  - Microsoft CAPI/CSP compliant crypto cards
  - PKCS#11 Cryptoki

PrivaSeal™ Signer - Tokens

- Other Hardware Tokens
  - USB token
  - Pentium III Processor Serial Number
- Soft Tokens
  - Windows Serial Number

PrivaSeal™ Verifier

- Click on Signature object to verify signature
  - Verifies signer's signature on the document
  - Verifies issuer's signature on the signing object
  - Verifies multiple signatures in signing order
- Viewing of Credentials and Certificates
  - Signer's Credentials
  - Signer's Certificate Chain
  - Issuer's Certificate Chain

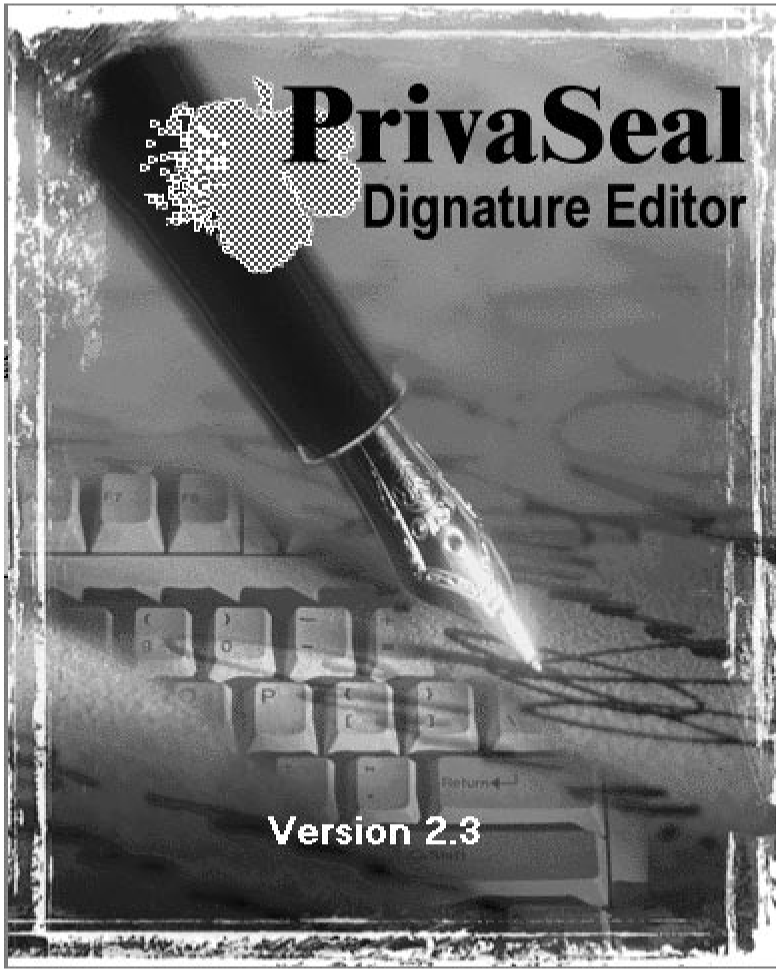
PrivaSeal^{TM} "Casual" PKI

- For internal use at reduced cost
  - X.509 for PrivaSeal Issuer only
  - PrivaSeal generated key pair for signers
- Encourages digital signature use where cost of full PKI implementation is not yet completely justified
- Provides scaleability to full PKI

PrivaSeal Summary

- Ease of Use
  - Drag and Drop
  - Incorporates easily into existing work practices
- Practical Orientation to PKI
  - PKI Friendly - Encourages early adoption at low cost
  - Supports corporate issuance of credentials with external CA issued certificates.
  - Supports full corporate PKI

Demonstration

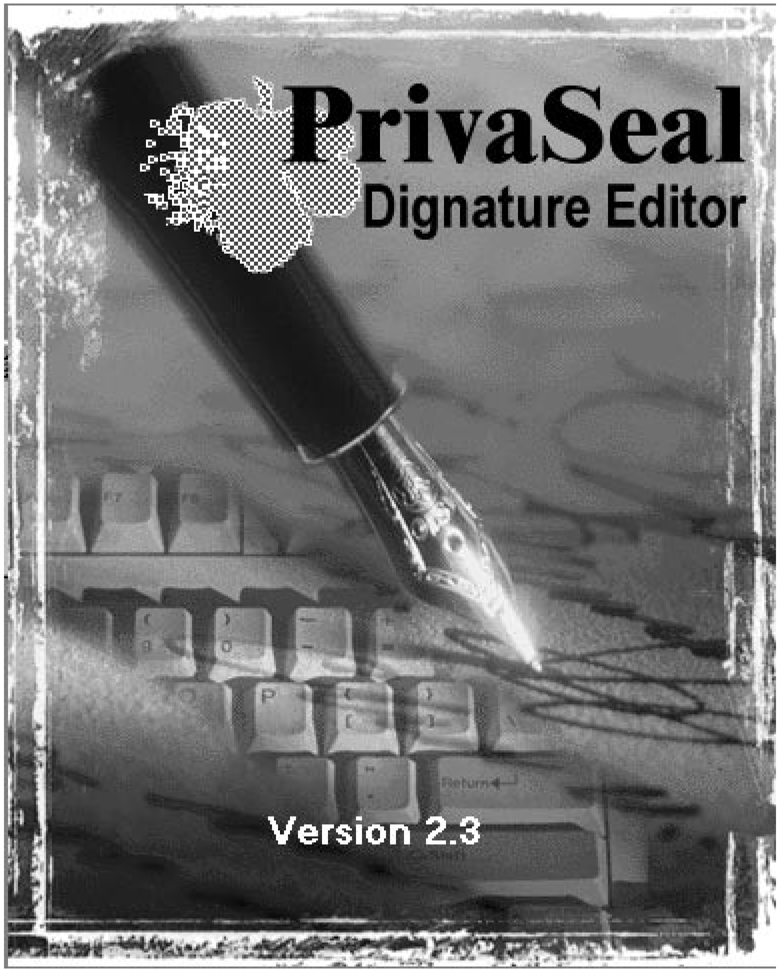


PrivaSeal Editor
PrivaSeal Signer
PrivaSeal Verifier

Enterprise Security and Document Content Assurance

Aliroo

Questions



Aliroo, Inc.
McLean, VA
703-917-0778

jprohaska@aliroo.com
dauman@aliroo.com

Enterprise Security and Document Content Assurance

Aliroo